08/04/00

UTILITY PATENT APPLICATION TRANSMITTAL
Under Small Entity Status
(New Nonprovisional Applications Under 37 CFR § 1.53(b))

Attorney Docket No.
0008-011P2

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Transmitted herewith is the patent application of ( ) application identifier or (X) first named inventor, <u>Peter M. Shipley</u>, entitled <u>Intelligent Network Security Device and Method</u>, for a(n):

( )   Original Patent Application.

(X)   Continuing Application (prior application not abandoned):
      (X)   Continuation   ( )   Divisional   ( )   Continuation-in-part (CIP)
      of prior application No: <u>09/210,057</u> Filed on: <u>12/10/1998</u>.
    (X)   A statement claiming priority under 35 USC § 120 has been added to the specification.

Enclosed are:
    (X)   Specification; <u>18</u> Total Pages.   (X) Drawing(s); <u>2</u> Total Sheets.
    (X)   Oath or Declaration:
      ( )   A Newly Executed Combined Declaration and Power of Attorney:
        ( ) Signed.   ( ) Unsigned.   ( ) Partially Signed.
      (X)   A Copy from a Prior Application for Continuation/Divisional (37 CFR § 1.63(d)).
        (X)   Incorporation by Reference. The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied, is considered as being part of the disclosure of the accompanying application and is hereby incorporated herein by reference.
        ( )   Signed Statement Deleting Inventor(s) Named in the Prior Application. (37 CFR § 163(d)(2)).
    ( )   Power of Attorney.   (X)   Return Receipt Postcard.
    ( )   Associate Power of Attorney.   (X)   A Check in the amount of $384.00 for the Filing Fee.
    ( )   Preliminary Amendment.   ( )   Information Disclosure Statement and Form PTO-1449.
    ( )   A Duplicate Copy of this Form for Processing Fee Against Deposit Account.
    ( )   A Certified Copy of Priority Documents (if foreign priority is claimed).
    ( )   Statement(s) of Status as a Small Entity.
    (X)   Statement(s) of Status as a Small Entity Filed in Prior Application, Status Still Proper and Desired.
    ( )   Other: _____ .

CLAIMS AS FILED				
FOR	NO. FILED	NO. EXTRA	RATE	FEE
Total Claims	8	0	$9.00	$ 0.00
Independent Claims	4	1	$39.00	$ 39.00
Multiple Dependent Claims (if applicable)				$0.00
Assignment Recording Fee				$0.00
Basic Filing Fee				$345.00
			Total Filing Fee	$ 384.00

Charge $_____ to Deposit Account _____ pursuant to 37 CFR § 1.25. At any time during the pendency of this application, please charge any fees required or credit any overpayment to this Deposit Account.

Respectfully submitted,

By: _Larry E. Henneman_
Larry E. Henneman, Jr., Reg. No.41,063

Date: 8/2/00

Correspondence Address:

Henneman & Saunders
121 E. 11th Street
Tracy, CA 95376
Phone: 209-833-8820
Fax: 209-833-8825

Attorney's File No: 16355-11C1
Applicant or Patentee: Peter M. Shipley
Serial/Patent Number: 09/210,057 Filed: December 10, 1998

VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS (37 CFR 1.9(f) AND 1.27(b) - <u>INDEPENDENT INVENTOR</u>

As a below-named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 CFR 1.9(c) for purposes of paying reduced fees reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled: **Intelligent Network Security Device and Method**

described in:

( )	the specification filed herein	
(x)	Application Serial No:	09/210,057
	filed:	December 10, 1998
( )	Patent No.:	_____
	issued:	_____

I have not assigned, granted, conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent inventor under 37 CFR 1.9(c) if that person had made the invention, or any concern which would not qualify as a small business concern under 37 CFR 1.9(d) or a nonprofit organization under 37 CFR 1.9 (e).

Each person, concern or organization to which I have assigned, granted, conveyed or licensed any rights in the invention is listed below:

(x)   no such person, concern or organization
( )   person, concern or organization listed below*

*NOTE: Separate Verified Statements are required for each named person, concern, or organization having rights to the invention averring to their status as small entities (37 CFR 1.27).

NAME: _____

ADDRESS: _____

( ) INDIVIDUAL   ( ) SMALL BUSINESS ( ) NONPROFIT ORGANIZATION

I acknowledge my duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the Issue Fee or any Maintenance Fee due after the date on which status as a small entity is no longer appropriate (37 CFR 1.28(b)).

Verified Statement (Independent Inventor)   Page 1

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful, false statements, false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this Verified Statement is directed.

SIGNATURES

Name of Inventor: Peter M. Shipley

Signature of Inventor: Date:

INTELLIGENT NETWORK SECURITY DEVICE AND METHOD
Peter M. Shipley

Cross Reference to Related Application

5   This application is a continuation of copending U.S. Patent Application Serial No. 09/210,057 filed 12/10/98, which is a continuation in part of U.S. Patent Application Serial No. 08//726,563 filed 10/7/96, now abandoned, both of which are incorporated herein by reference in their entirety.

TECHNICAL FIELD

10   The present invention relates to the field of computer security, and more particularly to a device and method for the prevention of unauthorized intrusion into computer networks and systems. The predominant current usage of the present inventive intelligent network security device and method is in the interface between local area networks and the internet.

BACKGROUND ART

       The need for network security today is beyond question. Not only are there thieves intent on stealing valuable data and putting it to their own misuse, computer networks must also be made secure against the many pranksters who would introduce viruses and generally try to cause trouble for reasons more arcane or obtuse.

       The need for simple security measures has been apparent essentially since the inception of computers. Before computers were hooked together into networks, physical security (keeping unauthorized users away from the computer) was generally deemed adequate. Passwords, often supplemented the physical security, were initially used as essentially the only means of computer based security, even after computers were linked together into private local and wide area networks. But the devious nature of the human mind is such that many view a locked door as a challenge rather than as a barrier which should not be passed. Inevitably, people with less than honorable intentions learned to bypass passwords and other such simple security devices. In response, improved security devices and methods were implemented and, in turn, in

response to that there were developed means and methods to defeat the improved security.

With the advent of the internet, the traditional security concerns have yet another aspect. When a computer system is connected to and interacting with the internet, it is no longer possible to deny access outright to the outside world, or to limit such access to a select few users with whom elaborate individual security measures can be taken. By definition, a computer network which interfaces with the internet is connected to every other computer and network on the internet. The only things preventing unauthorized access are the security measures employed by the individual networks. A rather thorough discussion of the need for and history of computer security is found in Computer Security Basics by Deborah Russell and G.T. Gangemi Sr., published by O'Reilly & Associates, Inc.

In short, in considering computer network security in relation to the internet, two of the important aspects are generally in opposition. Securing the confidentiality of data is important, but so is maintaining the availability of the network and data therein to authorized users. In a very narrow sense, the ultimate security would be to disconnect the network from the internet altogether. However, this usually is clearly an unsatisfactory repair, since it negates the useful purposes for which the network was connected to the internet in the first place. Indeed, to disrupt or disconnect the services provided by a network to users who might access it through the internet is, in many respects, to succumb to those "crackers" who would disrupt the effective security and/or operation of the network.

Within a network, various security measures can be put into place to create what is referred to as a "trusted" network. But there is no effective control over the rest of the world such that users accessing a local area network from without, as through the internet, can in any wise be trusted. One way to protect a trusted local area network without completely cutting off communication to the outside world is to set up a gateway computer (sometimes called a firewall) to isolate local users. Within the security perimeter of the local network, users may be able to communicate freely. However, all messages sent to or from users outside the local area network must pass through the firewall computer, or set of computers, which will check, route, and frequently label all

information that passes through it. A firewall can be a conventional computer running specific firewall software, or a dedicated computer device specifically constructed or configured as a firewall. The firewall can be dedicated solely to performing the firewall functions, or it can also perform additional functions such as packet routing, or the like,

5   in addition to its firewall functions.

As can be appreciated in light of the above discussion, there is no such thing as a completely secure system. The best that can be hoped for is to stay one step ahead of those persons who would circumvent existing security measures. Accordingly, those who use firewalls are consistently attempting to update the programming of the firewall

10   such that new methods for penetrating the firewall will be detected and abated. A well known recent program named "Satan", which was produced and made public by Dan Farmer, has a script of known methods by which network security can be breached, and Satan goes through this script attempting to break into a network. Satan was developed to perform a good faith security check on systems, and that is why it was made publicly

15   available. A program named "Gabriel" has been developed to recognize a Satan attack and to alert the system to such an attack. This is illustrative of the fact that a firewall can be programmed to recognize a known type of attack on the system. The firewall can also be programmed to block access to a recognized attacker.

To the inventor's knowledge, the firewall systems described above represent the

20   current state of the art in network security devices. Such firewalls are quite effective at detecting and blocking the particular types of network security breach attempts which are anticipated in the configuration and programming of the firewall. More specifically, such firewalls will block data packets according to the specific set of rules that is programmed into the firewall. Examples of such rules are; that a packet has to be

25   addressed to a valid machine on the network, that the packet cannot purport to be from a machine on the network, and that packet addresses cannot be any of the known invalid addresses.

Despite their effectiveness for their intended purpose, known prior art firewalls will not provide the sort of flexibility which may be needed in the future. In particular,

30   existing firewalls are not readily adaptable to provide a variety of responses based upon dynamically modified information. Moreover, existing firewalls are subject to

3

breach by any new and unique methods for circumventing security, at least until the programming of such a firewall is modified to block such new methods.

A U.S. Patent No. 5,606,668, issued to Shwed, teaches a method for easily programming a firewall. While Shwed provides a very useful invention, in that it allows

5   a firewall to be easily and quickly reprogrammed as necessary, it does not address the problem that it is litereally impossible to detect many sophisticated intrusion attempts by examining packets one at a time. That is, there may seemingly be nothing about any single packet which might alert an observer to the fact that something is amiss with a series of communications. Nor does Shwed teach or predict a controller which will

10   directly dynamically control a firewall without operator intervention. That is, although the Shwed invention provides a significant improvement, with the exception of the improved programming method, the invention taught by Shwed provides a programmed packet filter which is not different from the prior art.

DISCLOSURE OF INVENTION

15   Accordingly, it is an object of the present invention to provide a method and means for recognizing known and previously unknown types of attempts at breaching network security.

It is still another object of the present invention to provide a method and means

20   for controlling a network firewall to block sophisticated attempts at breaching network security.

It is yet another object of the present invention to provide a method and means for providing network security while also providing minimal interference with normal usage of the network.

25   It is still another object of the present invention to provide a method and means for intelligently controlling access to a computer network from outside sources.

It is yet another object of the present invention to provide a method and means for controlling network security which will see attempts to contact even "rogue" computers within a network, those being computers which are not specifically known to

30   a network administrator.

4

It is yet another object of the present invention to provide a network security means and method which uses artificial intelligence techniques, including adaptive pattern recognition, to recognize attempted security breaches.

It is still another object of the present invention to provide a network security
5   means and method which can provide an adaptable response appropriate to both the type of breach attempt and the source and quantity of such breach attempts.

Briefly, the preferred embodiment of the present invention is an intelligent network security device residing within a computer local area network, which device will examine information being communicated within the network. In an Ethernet system,
10   the device will examine data packets to recognize suspicious patterns of behavior. The device will be connected to control a firewall such that unauthorized or disruptive outside users will be blocked from accessing the network. Blocking will occur in several degrees, depending upon the assigned seriousness of a breach attempt, such that less serious perceived attempts will be allowed to continue to communicate with the network
15   at some level, or to resume communications after a period of time. The various degrees of blocking are provided such that perpetrators of inadvertent improprieties, and the like, will not be punished by absolute banishment from the system - which result would, itself, probably be an undesirable effect.

An advantage of the present invention is that each and every specific type of
20   attempt at breaching network security need not be known and anticipated.

A further advantage of the present invention is that interference with normal network traffic is minimal.

Yet another advantage of the present invention is that it can be used with existing computers, networks, and peripheral hardware.

25   Still another advantage of the present invention is that it is not dependent upon knowing the exact configuration of a network and/or the exact inventory of users on the network.

These and other objects and advantages of the present invention will become clear to those skilled in the art in view of the description of the best presently known
30   modes of carrying out the invention and the industrial applicability of the preferred

embodiments as described herein and as illustrated in the several figures of the drawing.

BRIEF DESCRIPTION OF DRAWINGS

5   Figure 1 is a diagrammatic view of a local area network incorporating an inventive intelligent network security device according to the present invention; and

Figure 2 is a flow diagram of an example of the inventive intelligent network security method.

10   ## BEST MODE FOR CARRYING OUT THE INVENTION

This invention is described in a preferred embodiment in the following description with reference to the Figures, in which like numbers represent the same or similar elements. While this invention is described in terms of the best mode for achieving this

15   invention's objectives, it will be appreciated by those skilled in the art that variations may be accomplished in view of these teachings without deviating from the spirit or scope of the present invention. For example, the present invention may be implemented using any combination of computer programming software, firmware or hardware. As a preparatory step to practicing the invention or constructing an apparatus according to

20   the invention, the computer programming code (whether software or firmware) according to the invention will typically be stored in one or more machine readable storage devices such as fixed (hard) drives, diskettes, optical disks, magnetic tape, semiconductor memories such as ROMs, PROMs, etc., thereby making an article of manufacture in accordance with the invention. The article of manufacture containing

25   the computer programming code is used by either executing the code directly from the storage device, by copying the code from the storage device into another storage device such as a hard disk, RAM, etc. or by transmitting the code on a network for remote execution. The method form of the invention may be practiced by combining one or more machine readable storage devices containing the code according to the

30   present invention with appropriate standard computer hardware to execute the code contained therein. An apparatus for practicing the invention could be one or more

computers and storage systems containing or having network access to computer program(s) coded in accordance with the invention, and the method steps of the invention could be accomplished by routines, subroutines, or subparts of a computer program product.

5   The inventive INSD is depicted in a diagrammatic view in Figure 1 and is designated therein by the general reference character 10. The INSD 10 is a part of a local area network ("LAN") 12 having a plurality of computers 14 (nine computers 14 are depicted in the example of Figure 1). The LAN 12 is connected to the internet 16 through a firewall 18. The computers 14, and other devices in the LAN 12 are

10   interconnected through a plurality of interconnecting data transmission media (such as wires, fiber optics, radio waves, and the like), and preferably wires 20, in the conventional manner.

      In the example of Figure 1, the best presently known embodiment 10 of the present invention has the LAN 12 using an Ethernet communication protocol and

15   configuration. However, this is not a necessary aspect of the invention, and it is anticipated that the inventive INSD 10 can be used, or adapted for use, with essentially any type of LAN 12 configuration. Also, while the LAN 12 is depicted, in the example of Figure 1, as being connected to the internet 16 through the firewall 18, the present invention is equally applicable to any situation where it is desired to isolate the LAN 12

20   from other devices by means of the firewall 18, as where the LAN 12 might be hard wired, or bridged, through the firewall 18 to another LAN (not shown), or other such variation.

      In the simplified example of Figure 1, a router 22 is shown interposed between some of the computers 14 and others of the computers 14 on the LAN 12. One skilled in

25   the art will recognize that other devices, such as bridges, hubs, and the like, are commonly used in Ethernet and other LAN network configurations. The router 22 is shown in the example of Figure 1 merely as a typical device which might, in some way, separate or segregate the computers 14 from other such devices on the LAN 12.

      The INSD 10 is positioned in the LAN 12 such that it will see all Ethernet packets

30   traveling through the firewall 18, whether such packets are directed into the LAN 12 from the internet 16 or from the LAN 12 into the internet 16. That is, the INSD 10 is

positioned in the LAN 12 such that the router 22, or other such devices as may be used in a particular LAN 12, will not filter or interfere with the ability of the INSD 10 to monitor traffic into and out of the entire LAN 12.

In the example of Figure 1, the inventive INSD 10 communicates directly with the firewall 18 through a serial cable 24 connected between a first serial port 26 of the INSD 10 and a second serial port 28 of the firewall 18. Although it would be possible, and within the scope of the present invention, to accomplish all communication between the INSD 10 and the firewall 18 through the interconnecting wires 20 of the LAN 12, the inventor believes that the use of the serial cable 24, as seen in the example of Figure 1, will provide more effective and simpler means of communication between the INSD 10 and the firewall 18.

Figure 2 is a flow diagram depicting an example of the best presently known embodiment of the inventive intelligent security method 30. As discussed previously herein, the inventive method 30 will be accomplished using software routines and may be physically embodied in a medium such as a floppy disk 31 (Fig. 1), CD ROM, or the like, for transport and for placing the code embodying the inventive method into the INSD 10. According to the intelligent network security method 30, the INSD 10 will monitor all Ethernet packets coming or going through the firewall 18 in a 'receive input, operation 32. It should be recognized that the 'receive input' operation 32 and, indeed, the entire intelligent network security method 30 will be repeated continuously during the operation of the INSD 10.

Following the receive input, operation 32, is a 'look for known code' operation 34. In the look for known code, operation 34, the INSD 10 will compare the data in each Ethernet packet to data known to be indicative of security breach attempts. It will be noted that this 'look for known code' operation 34 is, by itself, in many respects not unlike the known prior art method of examining data for known bits of code, packet addresses, or other data characteristics, to determine if a security breach is being attempted. However, the 'look for known code' operation 34 is generally distinguishable in that according to the present inventive method 30, the data packets are being examined and analyzed in essentially real time rather than by reference to log files.

As can be seen in the example of Figure 2, operating generally simultaneously with the 'look for known code' operation 34 in the best presently known embodiment 30 of the inventive method is a 'look for known patterns' operation 36. In the 'look for known patterns' operation 36, the INSD 10 will examine patterns of activity on the LAN 12. One skilled in the art will recognize that this will require that the INSD 10 retain certain data for a limited amount of time, as it is patterns of activity over time (as compared to a particular sequential data portion, itself) that is being examined here. While the inventor anticipates that many such patterns will be discovered and or developed as the inventive INSD 10 is put into widespread use, patterns which are now anticipated to be of interest include an ordered attempt to access each machine in a network. That is, many attempts to breach network security involve methodically going through each access point in a network looking for a "weak link". This pattern is relatively independent of the particular means that is being used to try to breach security at each such access port. Yet another example of the 'look for know patterns' operation 36 involves the fact that it can be known that certain types of commands will issue from certain types of users. When a command restricted to one type of user is followed by a command restricted (or generally associated with) another type of user - both coming from the same sender address - then a pattern of suspicious activity has been detected.

Another pattern which is considered to be of interest would be an attempt to access machines or access ports which do not exist. This would tend to indicate an outsider who does not actually know the configuration of the network. While a single, or even a few, such attempts might be indicative of an honest mistake, a great number of sequential attempts to access machines or access ports which do not exist would tend to indicate a real attempted security breach.

Yet another pattern which is considered to be of interest would be an attempt to access a port which is either not used at all or which is not used for the type of communication being attempt. Here, also, a small number of such attempts might be ignored (depending on the sensitivity of the data being protected) while a large number of such attempts would leave little doubt of a methodical attempt at intrusion.

Still another pattern which will be of interest will be a quantity of "responses" from machines on the internet 16 to which no corresponding inquiries have been sent from

the LAN 12. This would be indicative of a type of service blocking intrusion which has recently become popular. For example, a perpetrator might broadcast a signal through the internet 16 which falsely purports to come from the LAN 12. Subsequently, the multitude of responses (such as synchronization requests) forthcoming though the
5   internet 16 to the LAN 12 could completely tie up the LAN 12.

It should be noted that, in order for the 'look for known patterns' operation 36 to be successful, the INSD 10 might require some knowledge of the configuration of the LAN 12 (as illustrated by several of the examples above). This data can be stored in the memory of the INSD 10. While it is certainly possible that a network administrator could
10   manually update this data each time a change is made to the LAN 12 configuration, it is more practical and more likely that existing and future means for automatically determining the configuration of the LAN 12 will be employed to obtain such data for storage in and use by the INSD 10.

Following the 'look for known patterns' operation 36 and the 'look for known
15   code', operation 34 in the best presently known embodiment 30 of the inventive method is an 'assign weight to breach' operation 38. In the 'assign weight to breach' operation 38 an average of various factors (two factors, in the example of the best presently known embodiment 30 of the present inventive method) is computed. In the best presently known embodiment 30 of the present inventive method, one of the two factors
20   is the sensitivity of the data which an attempted security breach is trying to access. For example, if the data being protected is of only mid-level importance, then it might be assigned a value of "0.511 on a scale of '"10.011 to "11.011. The other factor used in the best presently known embodiment 30 of the present inventive method is the perceived sophistication of the attempted security breach. For example, if the perceived
25   attempted security breach were only questionably higher than an unartful attempt to legally access the system (such as, for example, entering the wrong "password three times in a row") then this factor might be given a weight of 110.211, and the assign weight to breach' operation 38 would assign an average of %'0.111 in this particular iteration of the inventive intelligent network security method 30.
30   It should be noted that the above factors and figures are given by way of example only. It is contemplated that network security administrators will discover many

factors that might or should be considered in the assign weight to breach, operation 38. It should also be noted that each of these factors might not be considered to be equally important, and so a weighted average might be used instead of the simple average used in the present example. Also, it is likely that some factors might be considered so

5 important as to require overriding the averaging process altogether. For example, if extremely sensitive data is concerned, any sort of perceived attempted security breach might be considered sufficient to completely shut down access to that data. In such an example, the 'assign weight to breach' operation 38 could be configured so as to provide an output value of "1.011 regardless of the value of other factors. Also, it might

10 be desirable to use a minimum value of 110.111 rather that "0.01 such that a lowest value of one factor would not set the average value to zero. Therefore, even if one factor were to be extremely low, then very high values of other factors could result in a high output value from the 'assign weight to breach' operation 38. It should also be noted that it is entirely within the scope of the present inventive method to use other

15 and/or more sophisticated calculations to decide the outcome provided in the example of the best presently known embodiment 30 of the present inventive method by the 'assign weight to breach' operation 38.

Following the assign weight to breach' operation is a 'react' operation 40. In the 'react' operation 40, the INSD 10 (Figure 2) will send a control signal to the firewall 18

20 via the serial cable 24. The control signal will direct the firewall 18 to take any of a number of prescribed actions, based upon the value assigned in the assign weight to breach' operation (or variations thereof, as described above or such as may be developed in the future).

It should be noted that the above operations differ considerably from the prior art

25 in respects including that the firewall 28 is dynamically programmed, in essentially real time, according to a number of factors. Therefore, the firewall 28 is enabled to provide an appropriate response and, as described above, to change that response according to factors deemed appropriate. This is as compared to a prior art firewall which, no matter how sophisticated it's programming, can only accept or reject packets according

30 to such programming and cannot, as in the example provided herein, reject packets

according to other more sophisticated criteria as described by way of example hereinafter.

An example of the various actions which it is anticipated might be directed in the 'react' operation 40 is to block all access to the LAN 12 from a sender which has been
5   detected as attempting the security breach. Another example would be to disallow access from such a sender for a prescribed period of time only. Yet another example would be to disallow access by such a user only to specific machines or blocks of data within the LAN 12. More extreme examples would be to completely shut down access to a block of data, or even to the entire LAN 12, by any user until the network administrator
10 has time to evaluate the security breach and take appropriate action. Different variations and/or combinations of these outcomes will be situationally appropriate for application in the 'react' operation 40.

A variation of the 'react' operation 40 which could be used instead of, or in addition to, that described previously herein would have the INSD 10 send a signal
15 through the interconnecting wires 20 out through the firewall 18 to devices on the internet 16. An example would be to send a reset signal to a device in the internet 16 that was, itself, sending a disruptive signal or an excess of data to the LAN 12. This would be particularly appropriate where an innocent sender has been tricked to send such disruptive communications, as described in an example discussed in relation to
20 the prior art herein.

It should be noted that the best presently known embodiment 30 of the intelligent network security method has been illustrated herein as a generally linear process which operates generally continuously and repeatedly as incoming data packets are received on the LAN 12. In this example, variations in outcome are achieved by assigning
25 weights or values to certain perceived factors. One skilled in the art will be aware that a similar outcome could be achieved by programming the INSD 10 to operate according to a branching method wherein different perceived situations (such as a recognized pattern of activity) could cause the decision making within the INSD 10 to branch accordingly.

30 The present invention is susceptible to numerous modifications and additions. For example, as touched upon briefly previously herein, it is anticipated by the inventor

12

that network security administrators will discover a great many factors which should be weighed in the assign weight to breach, operation 38. Similarly, it is anticipated that outcomes and actions in addition to those specifically discussed herein will be utilized in the 'react' operation.

5   It is also anticipated that other broad categories of detection operations will be utilized in the future, in addition to the 'look for known code' operation 34 and the 'look for known patterns' operation which are specifically set forth herein as being a part of the best presently known embodiment 30 of the present inventive method.

10   **INDUSTRIAL APPLICABILITY**

The inventive intelligent network security device and method are intended to be widely used for improving security in computer systems and networks which are connected to telephonic or other data transfer means such that there is a potential for intrusion into the protected network through such data transfer means.

15   While the primary anticipated application is in the protection of networks which can be accessed via telephone lines and/or other communications means which provide access to the internet, the present invention is applicable to essentially any situation where it is desired to protect data within a secure computer system from unauthorized or improper access from the outside.

20   A particular benefit of the present invention is that it is readily adaptable to deal with new and unique means for attempting to breach network security. Indeed, it is anticipated by the inventor that the INSD 10 can be caused to be self learning, in at least some respects, as artificial intelligence is developed relating to network security.

It should be noted that the present inventive INSD 10 will require a considerable

25   amount of processing power for its optimal effectiveness, particularly where a great deal of incoming data must be processed and analyzed. However, it should also be noted that, according to the present inventive method 30, the firewall 16 need not have a great deal of processing power because it will generally only be carrying out relatively simple instructions provided from the INSD 10.

30   It is anticipated by the inventor that future modifications of the INSD 10 and the intelligent network security method 30 might cause the INSD 10 to actually look outward

from the LAN 12 into the internet 16 to analyze and discover information about potential breachers of security.

Yet another anticipated modification of the best presently known embodiment 30 of the present inventive method would have the INSD 10 look at data outgoing from the

5   LAN 12 into the internet 16 to look for "inappropriate" outgoing responses or messages from the protected LAN 12.

It should be noted that an element of the present invention is that it looks at patterns of activity over time. The term "over time" is herein specifically defined to mean over a time period which includes the examination of a series of more than one

10   packet, whereby patterns of activity can be detected. For example, different types of users might make different types of requests of a system. Where a packet having characteristics that might typically be sent only by a lower level user is followed by a packet having characteristics that might typically be sent only by a higher level user, it might be assumed that something is amiss. This is true even where both packets

15   might, in and of themselves, be perfectly acceptable such that no system in the prior art could have detected the problem.

Since the intelligent network security device and method may be readily produced and integrated into existing computer networks, and will work in conjunction with existing and anticipated network firewall devices with minimal modifications, and

20   since the advantages as described herein are provided, it is expected that the intelligent network security device and method will be readily accepted in the industry. For these and other reasons, it is expected that the utility and industrial applicability of the invention will be both significant in scope and long lasting in duration.

While the usefulness of the present invention is not limited to recognizing

25   patterns of activity over time, this is a clear distinction of the present invention over the prior art. Patterns such as systematic attempts to break a security code can be recognized and a message sent to the firewall to stop (permanently or temporarily) accepting input from the suspected source and/or other security measures can be initiated. One particular problem with the prior art that is thus addressed according to

30   the present invention involves the fact that Unix based systems replace data in packets with the newer of overlapping data. Clever "crackers" have used this fact to sneak

through instructions that simply cannot be stopped by conventional "static" firewall/packet filter devices. An additional aspect of the ability of the present invention to dynamically detect patterns of behavior and control the firewall accordingly, is that security rules can be stated in broad terms of behavior such that attempts to crack

5   security which are not specifically anticipated (new and clever ways of breaking in) can be stopped. The term "control the firewall" is herein specifically defined to mean sending instructions to the firewall to direct it to reject packets which would not otherwise be rejected, given whatever programmed instructions are already existant in the firewall prior to the exercise of such "control". That is, while the "rules" that are

10 programmed in to conventional firewall systems (such as those programmed in according to the inventive method of the Shwed patent, cited previously herein) can effectively define what sorts of packets will be admitted to a network - in terms of addresses, imbedded codes, and many other criteria, these can all be duplicated by a sufficiently clever cracker to circumvent security. However, attempts at such

15 circumvention will generally be characterized by a pattern of activity which can be detected according to the present invention, and the proper action can be taken automatically by the controller without immediate operator intervention. The "proper action" can include (but will not be limited to) the permanent rejection of all packets sent from a user, the temporary rejection of such packets, or – as in the case of a detected

20 deliberate breach of a high security system – the shutting down of communications to that system entirely until the nature and source of the breach can be more fully analyzed.

All of the above are only some of the examples of available embodiments of the present invention. Those skilled in the art will readily observe that numerous other

25 modifications and alterations may be made without departing from the spirit and scope of the invention. Accordingly, the above disclosure is not intended as limiting and the appended claims are to be interpreted as encompassing the entire scope of the invention.

I CLAIM:

1   1.   In a computer system connected to an external communications medium, a

2   security device comprising:

3   a programmable firewall device interposed between the computer system and

4   the external communications medium;

5   a controller device configured within the computer system such that said

6   controller device can access all communications into and out of the computer system

7   and can control the firewall to block communications between the computer system and

8   the external communications medium when an attempted security breach is detected;

9   a communications device for communicating instructions from said controller

10   device to said firewall device for controlling said firewall device; wherein

11   said controller device examines communications incoming to the computer

12   system to detect attempted security breaches; and

13   the controller device continuously controls the firewall during the operation of the

14   computer system to block communications between the computer system and the

15   external communications medium when an attempted security breach is detected.

1   2.   A computer program product which includes codes on a computer readable

2   medium wherein codes are being executed by a computer system, comprising:

3   a detect code operation performed by the codes on the computer readable

4   medium wherein known improper code is detected; and

5   a detect patterns operational routine performed by the codes on the computer

6   readable medium wherein a pattern of activity is detected over time.

1   3.   The computer program product of claim 2, and further including:

2   a weighting operation performed by the codes on the computer readable medium

3   wherein a weight is assigned to a detected security breach.

16

1   4.   The computer program product of claim 2, wherein:

2   a firewall is automatically reprogrammed by the codes on the computer readable

3   medium.

1   5.   A computer program product which includes codes on a computer readable

2   medium wherein codes are being executed by a computer system, comprising:

3   at least one detect operation performed by the codes on the computer readable

4   medium wherein a computer security breach is detected; and

5   a weighting operation performed by the codes on the computer readable medium

6   wherein a weight is assigned according to the importance of the security breach.

1   6.   The computer program product of claim 5, and further including:

2   a react operation performed by the codes on the computer readable medium

3   wherein a firewall is reprogrammed in real time to react to the security breach.

1   7.   A computer program product which includes codes on a computer readable

2   medium wherein codes are being executed by a computer system, comprising:

3   at least one detect operation performed by the codes on the computer readable

4   medium wherein a computer security breach is detected; and

5   a react operation performed by the codes on the computer readable medium

6   wherein a firewall is reprogrammed in real time to react to the security breach.

1   8.   The computer program product of claim 7, wherein:

2   said react operation reprograms the firewall according to an assigned weight, the

3   assigned weight being a function of the type of security breach detected.

17

0008-011P2

ABSTRACT

An intelligent network security device ("INSD") (10) operates in a local area network ("LAN") (12) according to an intelligent network security method (30). The LAN (12) has a plurality of computers (14) and connects to the internet (16) through a firewall (18). The INSD (10) resides within the LAN (12) such that data traversing between the LAN (12) and the internet (16) is accessible thereto. The INSD (10) looks for code and patterns of behavior and assigns a value to perceived attempted security breaches. The INSD (10) then directs the firewall (16) to take any of a prescribed plurality of actions, based upon such value.

18

Fig. 1

firewall 18

28

24

INSD 10

26

router 22

computer 14

computer 14

computer 14

computer 14

computer 14

computer 14

computer 14

computer 14

computer 14

16

31

20

12

Fig. 2

30

```
          ┌─────────────┐
   32 ───→│   receive   │
          │    input    │
          └──────┬──────┘
                 │
        ┌────────┴────────┐
        ↓                 ↓
┌───────────────┐  ┌──────────────────┐
│   look for    │  │     look for      │
│  known code   │  │  known patterns   │
└───────┬───────┘  └────────┬─────────┘
   34   │                   │    36
        └────────┬──────────┘
                 ↓
        ┌─────────────────┐
        │  assign weight  │── 38
        │   to breach     │
        └────────┬────────┘
                 ↓
        ┌─────────────────┐
        │     react       │── 40
        └─────────────────┘
```

DECLARATION, POWER OF ATTORNEY AND PETITION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled "**Intelligent Network Security Device and Method**" the specification of which

        ☐   is attached hereto
        ☒   was filed on December 10, 1998 as Application Serial No. 09/210,057
            and was amended on _____

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application of which priority is claimed.

Prior Foreign Application(s)

Priority Claimed

(Number)	(Country)	(Day, month, year filed)	Yes	No
(Number)	(Country)	(Day, month, year filed)	Yes	No
(Number)	(Country)	(Day, month, year filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

08/726,563	October 7, 1996	Pending
(Application Serial No.)	Filing Date	(Status: Patented, pending, abandoned)

(Application Serial No.)	Filing Date	(Status: Patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.
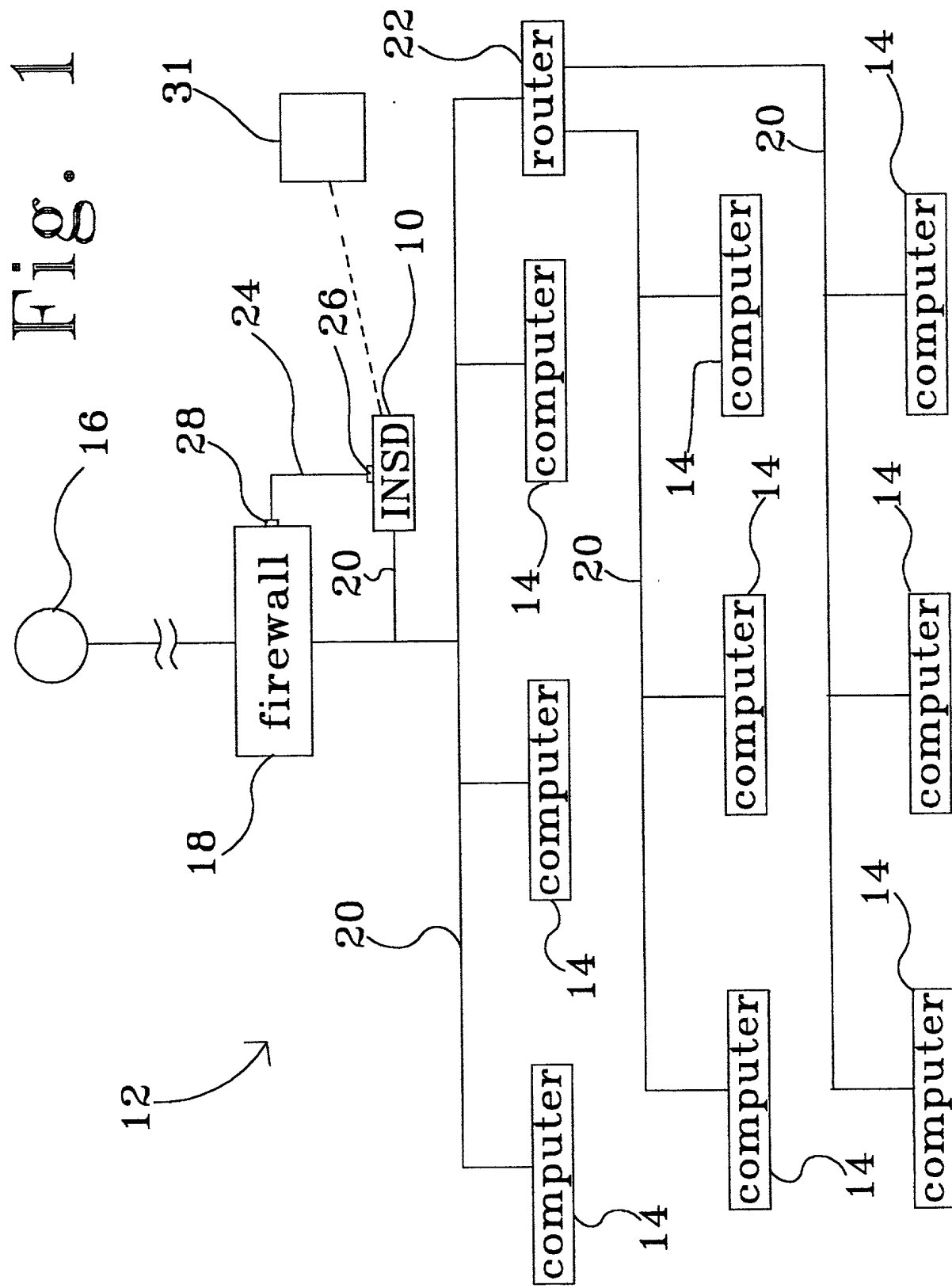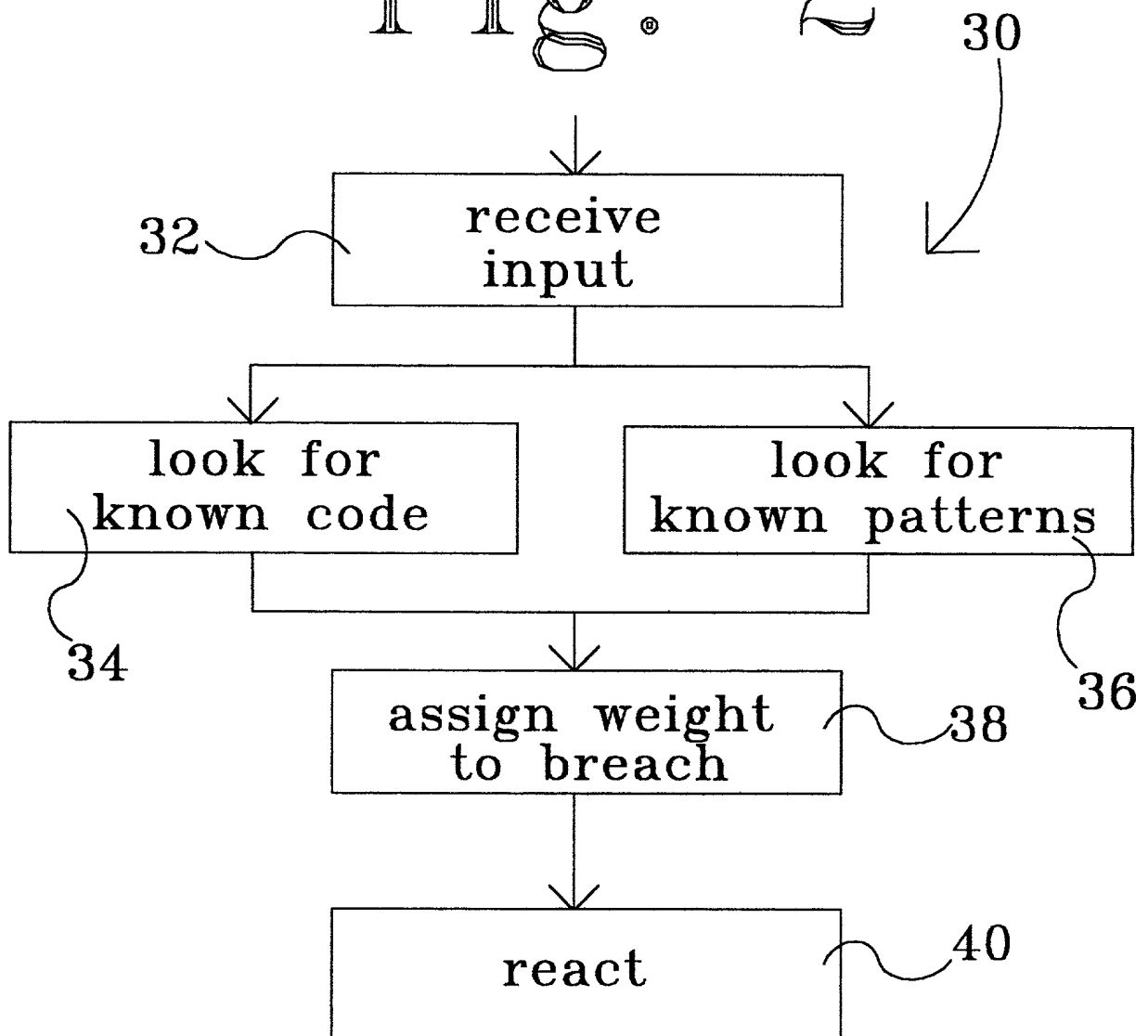
And I hereby appoint W. POMS, Reg. 18,782; G.P. SMITH, Reg. 20,142; G.E. LANDE, Reg. 22,222; A.C. ROSE, Reg. 17,047; L.J. BOVASSO, Reg. 24,075; D.J. OLDENKAMP, Reg. 29,421; C. DARROW, Reg. 30,166; M.E. HARRIS, Reg. 26,690; K.A. MACLEAN, Reg. 31,118; C. ROSENBERG, Reg. 31,464; M.E. BROWN, Reg. 28,590; E.F. O'CONNOR, Reg. 25,903; R.F. CARR, Reg. 17,110; A. ROTHENBERG, Reg. 17,843; R.L. GAUSEWITZ, Reg. 16,960; M.A. KONDZELLA, Reg. 18,013; A.P. BLOCK, Reg. 35,450; S.R. HANSEN, Reg. 38,486; D.N. LARSON, Reg. 29,401; J.W. INSKEEP, Reg. 33,910; G.F. COTTERELL, Reg. 37,802; H.D. JASTRAM, Reg. 19,777; J.M. KALIS, Reg. 37,650; C.J. LERVICK, Reg. 35,244; C.A.S. HAMRICK, Reg. 22,586; R.O. GUILLOT, Reg. 28,852; E.C. CHANG, Reg. 37,593; J.D.

VOELZKE, Reg. 37,957; G.L. FOUNTAIN, Reg. 36,374; J. BOYCE, Reg. 40,920; C. CHOU, Reg. 41,672; L. HENNEMAN, Reg. 41,063; M. IMAN, Reg. 38, 190; OPPENHEIMER WOLFF & DONNELLY LLP, Ten Almaden Boulevard, Suite 600, San Jose, California 95113, (408) 795-3000, as my attorneys with full power of substitution and revocation, to prosecute said application and to transact in connection therewith all business in the Patent and Trademark Office and before competent International Authorities.

Address all telephone calls to Justin F. Boyce at (408) 795-3000 and address all correspondence to:

Justin F. Boyce, Esq.
OPPENHEIMER WOLFF & DONNELLY LLP
10 Almaden Boulevard, Suite 600
San Jose, California 95113

Wherefore I pray that Letters Patent be granted to me for the invention or discovery described and claimed in the foregoing specification and claims, and I hereby subscribe my name to the foregoing specification and claims, declaration, power of attorney, and this petition.

Full Name of Sole or First Inventor:	Peter M. Shipley
Home Address:	2650 Bancroft Way #51. Berkeley. CA 94704-1700
Post Office Address:	Same as above
Citizenship:	United States
Inventor's Signature:	_____ Date: 1/20/99